GENETIC ALGORITHM FOR AUDIO WATERMARKING

Miss Nidhi G. Gupta[1] (M.E. Scholar), Dr. S. A. Ladhake[2] (Principal)
Computer Science & Engineering, Sipna College of Engineering & Technology
Amravati, Maharashtra, India.

Abstract: This paper presents, genetic algorithm for principled approach to resolve the remained problems of substitution technique of audio watermarking. Using the proposed genetic algorithm, message bits are embedded into multiple, vague and higher LSB layers, resulting in increased robustness. . The basic idea of this paper is to present methods that hide information in cover audio using Least Significant Bit (LSB) coding method along with encryption so as to increase the security the robustness specially would be increased against those intentional attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well. It is mainly required for increasing security in transferring and archiving of audio files

Keywords: data hiding, substitution techniques, audio watermarking, artificial intelligence, genetic algorithm.

I. INTRODUCTION

During the early to mid-1990s, digital watermarking attracted the attention of a significant number of researchers after several early works that may also be classified as such [11]. Since then the number of publications has increased exponentially to several hundred per year. It started from simple approaches presenting the basic principles to sophisticated algorithms using results from communication theory and applying them to the watermarking problem [12, 20, 21, 22, 23, and 24]. Digital watermarking has been proposed as a new, alternative method to enforce the intellectual property rights and protect digital media from tampering. It involves a process of embedding into a host signal a perceptually transparent digital signature, carrying a message about the host signal in order to "mark" its ownership. The digital signature is called the digital watermark. The digital watermark contains data that can be used in various applications including digital rights existence of the watermark is indicated when watermarked media is passed through an appropriate watermark detector. A watermark, which usually consists of a binary data sequence, is inserted into the host signal in the watermark embedder. Thus, a watermark embedder has two inputs; one is the watermark message (usually accompanied by a secret key) and the other is the host signal (e.g. image, video clip, audio sequence etc.). The output of the watermark embedder is the watermarked signal, which cannot be perceptually discriminated from the host signal. The watermarked signal is then usually recorded or broadcasted and later presented to the watermark detector. The detector determines whether the watermark is present in the tested multimedia signal, and if so, what message is encoded in it. Various types of watermarks can be categorized due to their different properties. Robust watermarks are designed to resist against heterogeneous manipulations; all applications presupposing security of the watermarking systems require this type of watermark. Fragile watermarks are embedded with very low robustness. Therefore, this type of watermark can be destroyed even by the slightest manipulations. In this sense they are comparable to the hidden messages in Journal of Information Assurance and Security 5 (2010) 102-111 Received October 10, 2009 1554-1010 $ 03.50 Dynamic Publishers, Inc. steganography methods. They can be used to check the integrity of objects. Public and private watermarks are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve markings. According to the basic principle of watermarking, the same key is used in the encoding and decoding process. If the key is known, this type of watermark is referred to as public, and if the key is hidden, as private watermarks. Public watermarks can be used in applications that do not have security-relevant requirements (e.g., for the embedding of meta information).Visible or localized watermarks can be logos or overlay images in the field of image or video watermarking. Due to the implicit localization of the information, these watermarks are not robust.

Watermarking algorithms can be characterized by a number of defining properties. Three of them, which are most important for audio watermarking algorithms, are defined below.

Transparency evaluates the audible distortion due to signal modifications like message embedding or attacking. In order to meet fidelity constraint of the embedded information, the perceptual distortion introduced due to embedding should be below the masking threshold estimated based on the HAS/HVS and the host media

Capacity of an information hiding scheme refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion in the marked media.

Robustness measures the ability of embedded data or watermark to withstand against attack generally include common data manipulations such as lossy compression, digital-to-analog conversion, re-sampling, re-quantization, etc. whereas intentional attacks cover a broad range of media degradations which include addition white and colored noise, rescaling, rotation (for image and video steganography schemes), resizing, cropping, random chopping, and filtering attacks.

II. REQUIREMENTS AND DESIGN

According to the intended application of watermarks in audio data, the algorithm as well as the watermark itself has to fulfill a set of requirements [15]. The IFPI has specified the desired features of an optimal audio watermarking method. These requirements can be elaborated and subdivided further into signal processing properties, security properties, and application-specific requirements of the algorithm and the watermark.103 Zamani et al. Quality and robustness are related to the properties of the watermarked tracks and the embedded watermarks, and are general requirements for all watermarking systems. Nevertheless the ranking of these two requirements is special in the audio case (see below). The catalogues of possible audio signal manipulations depending on the application contains but are not limited to the following signal manipulations, which can be grouped into different categories.

A. Removal manipulations and attacks

- Addition of multiplicative and additive noise;
- Filtering like low-, high-, and all pass filtering;
- Lossy compression, for example, MPEG audio layer I, II, III;
- Noise reduction applying different kinds of algorithms;
- Digital to analog (D/A) and analog-to-digital (A/D) conversion;
- Changing the sampling rate (i.e., quantization of the audio track);
- Collusion and statistical attacks.

B. Misalignment manipulations and attacks

• Fluctuating time and pitch scaling;
• Cropping or insertion of samples. Beside s removal and misalignment, embedding and detection attacks can be applied as in all other watermarking domains. In addition to the general requirements of the quality of the watermarked copies and the robustness and security of the embedded watermarks, applications like active broadcast monitoring and customer identification for transaction tracking extend the range of the necessary features of the underlying algorithm. Both types of applications have in common the fact that the watermark is a function of time only known right before the time of delivery. Therefore, the speed of the watermark encoder is of vital importance for the applicability of the watermarking techniques. Even for real-time watermarking systems, the need to embed a large number of different watermarks simultaneously is a critical issue. The requirements detailed above describe the maximum sets of criteria an audio watermarking algorithm has to fulfill. Since the described features can in general not be fulfilled simultaneously in each imaginable application, different variations and corresponding design criteria are relevant for the development of an effective method. The most important requirement addresses the quality of the watermarked audio tracks. If the quality of the audio tracks cannot be preserved, neither users (whether consumers or broadcast industry professionals) nor especially the recording industry will accept this technology. This emphasizes the priority in ranking among the requirements from quality (first) to robustness (second) and data capacity (third). To ensure the quality of the watermarked audio tracks, a psychoacoustic model has to be an integral part of the watermark encoder. Modern advances in computer, communication and signal processing have enabled the discovery of sophisticated techniques of steganography. These advances have broadened steganography's use to include various types of medium and various forms of information. The developed techniques allow text, audio, video, graphics, or codes to be concealed in electronic documents containing text, graphics, and images and even in electronic audio or video files. Steganography has numerous applications like digital rights management, access control, covert communication, annotation etc.

III. WATERMARKING APPLICATIONS

Obviously, the most significant applications of data hiding are covert communication. Several application areas for digital watermarking are introduced below.

Ownership protection: In the ownership protection applications, a watermark containing ownership information is embedded to the multimedia host signal. The watermark, known only to the copyright holder, is expected to be very robust and secure (i.e., to survive common signal processing modifications and intentional attacks), enabling the owner to demonstrate the presence of this watermark in case of dispute to demonstrate his ownership. Watermark detection must have a very small false alarm probability. On the other hand, ownership protection applications require a small embedding capacity of the system, because the number of bits that can be embedded and extracted with a small probability of error does not have to be large.

Proof of ownership: It is even more demanding to use watermarks not only in the identification of the copyright ownership, but as an actual proof of ownership. The problem arises when adversary uses editing software to replace the original copyright notice with his own one and then claims to own the copyright himself. In the case of early watermark systems, the problem were that the watermark detector was readily available to adversaries anybody that can detect a watermark can probably remove it as well. Therefore, because an adversary can easily obtain a detector, he can remove owner’s watermark and replace it with his own. To achieve the level of the security necessary for proof of ownership, it is indispensable to restrict the availability of the detector. When an adversary does not have the detector, the removal of a watermark can be made extremely difficult. However, even if owner’s watermark cannot be removed, an adversary might try to undermine the owner. As described in [15], an adversary, using his own watermarking system, might be able to make it appear as if his watermark data was present in the owner’s original host signal. This problem can be solved using a slight alteration of the problem statement. Instead of a direct proof of ownership by embedding e.g. "Dave owns this image" watermark signature in the host image, algorithm will instead try to prove that the adversary’s image is derived from the original watermarked image. A Novel Approach for Audio Watermarking 104 Such an algorithm provides indirect evidence that it is more probable that the real owner owns the disputed image, because he is the one who has the version from which the other two were created.

Authentication and tampering detection: In the content authentication applications, a set of secondary data is embedded in the host multimedia signal and is later used to determine whether the host signal was tampered. The robustness against removing the watermark or making it undetectable is not a concern as there is no such motivation from attacker's point of view. However, forging a valid authentication watermark in an unauthorized or tampered host signal must be prevented. In practical applications it is also desirable to locate (in time or spatial dimension) and to discriminate the unintentional modifications (e.g. distortions incurred due to moderate MPEG compression [12]) from content tampering itself. In general, the watermark embedding capacity has to be high to satisfy the need for more additional data than in ownership protection applications. The detection must be performed without the original host signal because either the original is unavailable or its integrity has yet to be established. This kind of watermark detection is usually called a blind detection.

Fingerprinting: Additional data embedded by watermark in the fingerprinting applications are used to trace the originator or recipients of a particular copy of multimedia file. For example, watermarks carrying different serial or identity (ID) numbers are embedded in different copies of music CDs or DVDs before distributing them to a large number of recipients. The algorithms implemented in fingerprinting applications must show high robustness against intentional attacks and signal processing modifications such as lossy compression or filtering. Fingerprinting also requires good anti-collusion properties of the algorithms, i.e. it is not possible to embed more than one ID number to the host multimedia file, and otherwise the detector is not able to distinguish which copy is present. The embedding capacity required by fingerprinting applications is in the range of the capacity needed in copyright protection applications, with a few bits per second.

Broadcast monitoring*:* A variety of applications for audio watermarking are in the field of broadcasting. Watermarking is an obvious alternative method of coding identification information for an active broadcast monitoring. It has the advantage of being embedded within the multimedia host signal itself rather than exploiting a particular segment of the broadcast signal. Thus, it is compatible with the already installed base of broadcast equipment, including digital and analogue communication channels. The primary drawback is that embedding process is more complex than a simple placing data into file headers. There is also a concern, especially on the part of content creators, that the watermark would introduce distortions and degrade the visual or audio quality of multimedia. A number of broadcast monitoring watermark-based applications are already available on commercial basis. These include program type identification, advertising research, broadcast coverage research etc. Users are able to receive a detailed proof of the performance information that allows them to:

- Verify that the correct program and its associated promos aired as contracted;
- Track barter advertising within programming;
- Automatically track multimedia within programs using automated software online.

IV. ALGORITHMS

Watermarking algorithms were primarily developed for digital images and video sequences; interest and research in audio watermarking started slightly later. In the past few years, several algorithms for the embedding and extraction of watermarks in audio sequences have been presented. All of the developed algorithms take advantage of the perceptual properties of the human auditory system (HAS) in order to add a watermark into a host signal in a perceptually transparent manner. A broad range of embedding techniques goes from simple least significant bit (LSB) scheme to the various spread spectrum methods. The overview given in this section presents the best known general audio watermarking algorithms, with an emphasis on the algorithms that were used as a basis for published work (LSB algorithm, spread spectrum, improved spread spectrum, etc).

Least Significant Bit (LSB) Coding : One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. For example if we want to hide the letter „A‟ (binary equivalent **1000001**) into a digitized audio file where each sample is represented with 16 bits, then LSB of 7 consecutive samples (each of 16 bit size) is replaced with each bit of binary equivalent of the letter „A‟ [10]. Advantages: It is the simplest way to embed information in a digital audio file. It allows large amount of data to be concealed within an audio file, use of only one LSB of the host audio sample gives a capacity equivalent to the sampling rate which could vary from 8 kbps to 44.1 kbps (all samples used) [11]. This method is more widely used as modifications to LSBs usually not create audible changes to the sounds. Disadvantage: It has considerably low robustness against attacks.

Parity Coding: Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner. Disadvantage: This method like LSB coding is not robust in nature.

Phase Coding: Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. It "works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments".

Disadvantage: It is a complex method and has low data transmission rate.

Spread Spectrum (SS)*:* It attempts to spread out the encoded data across the available frequencies as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file is frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. Advantage: It offers moderate data transmission rate while maintaining a high level of robustness. Disadvantage: It can introduce noise into a sound file.

Echo data hiding: Text can be embedded in audio data by introducing an echo to the original signal. The data is then hidden by varying three parameters of the echo: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded.

V. GENETIC ALGORITHM APPROACH

As Figure 1 shows, there are four main steps in this algorithm that are explained below.

Alteration: At the first step, message bits substitute with the target bits of samples. Target bits are those bits which place at the layer that we want to alter. This is done by a simple substitution that does not need adjustability of result be measured.

Modification*:* In fact this step is the most important and essential part of algorithm. All results and achievements that we expect are depending on this step. Efficient and intelligent algorithms are useful here. In this stage algorithm tries to decrease the amount of error and improve the transparency. For doing this stage, two different algorithms will be used. One of them that is more simple likes to ordinary techniques, but in aspect of perspicacity will be more efficient to modify the bits of samples better. Since transparency is simply the difference between original sample and modified sample, with a more intelligent algorithm, I will try to modify and adjust more bits and samples than some previous algorithms. If we can decrease the difference of them, transparency will be improved. There are two example of adjusting for expected intelligent algorithm below. Sample bits are: 001**0**1111 = 47 Target layer is 5, and message bit is 1 Without adjusting: 001**1**1111 = 63 (difference is 16) After adjusting: 001**1**0000 = 48 (difference will be 1 for 1 bit embedding) 109 Zamani et al. Sample bits are: 001**00**111 = 39 Target layers are 4&5, and message bits are 11 Without adjusting: 001**11**111 = 63 (difference is 24) After adjusting: 000**11**111 = 31 (difference will be 8 for 2 bits embedding) Another one is a Genetic Algorithm which the sample is like a chromosome and each bit of sample is like a gene. First generation or first parents consist of original sample and altered sampled. Fitness may be determined by a function which calculates the error. It is clear, the most transparent sample pattern should be measured fittest. It must be considered that in crossover and mutation the place of target bit should not be changed.

Verification*:* In fact this stage is quality controller. What the algorithm could do has been done, and now the outcome must be verified. If the difference between original sample and new sample is acceptable and reasonable, the new sample will be accepted; otherwise it will be rejected and original sample will be used in reconstructing the new audio file instead of that.

Reconstruction*:* The last step is new audio file (stego file) creation. This is done sample by sample. There are two states at the input of this step. Either modified sample is input or the original sample that is the same with host audio file. It is why we can claim the algorithm does not alter all samples or predictable samples. That means whether which sample will be used and modified is depending on the status of samples (Environment) and the decision of intelligent algorithm.

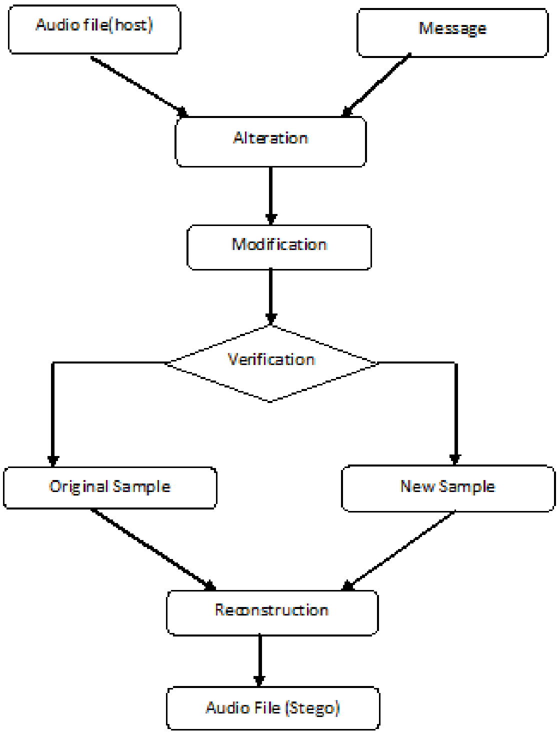

Figure 1: Approach Diagram

VI. CONCLUSIONS

Besides some other papers about applying GA for watermarking purpose [7, 8, 9, 10], a new approach is proposed to resolve two problems of substitution technique of audio watermarking. First problem is having low robustness against attacks which try to reveal the hidden message and second one is having low robustness against distortions with high average power. An intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness.

REFERENCES

[1] Cvejic N. and Seppänen T. ”Increasing the capacity of LSB based audio steganography”, Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2002, pp. 336- 338.

[2] Fridrich, Jessica and others. “Steganalysis of LSB Encoding in Color Images.” Proceedings of the IEEE International Conference on Multimedia and Expo. 1279– 1282. New York: IEEE Press, 2000.

[3] Lee, Y. K. and Chen L. H. “High Capacity Image Steganographic Model”. IEEE Proceedings Vision, Image and Signal Processing, pp. 288-294, 2000.

[4] Martín Alvaro, Sapiro Guillermo and Seroussi Gadiel, “Is Image Steganography Natural?” IEEE Transactions On Image Processing, Vol. 14, No. 12, December, 2005.

[5] Pal S.K., Saxena P. K. and Mutto S.K. “The Future of Audio Steganography”. Pacific Rim Workshop on Digital Steganography, Japan, 2002.

[6] Westfeld A. and Pitzmann A. "Attacks on Steganographic Systems". Lecture Notes in Computer Science, vol. 1768, Springer-Verlag, Berlin, pp. 61-75, 2000.

[7] Huang Cheh Huang, Chi-Ming Chu and Jeng-Shyang Pan, “The optimized copyright protection system with genetic watermarking”, 2009, pp. 333-343, 2009.

[8] Shahreza S.S. and Shalmani M.T.M., “Adaptive wavelet domain audio steganography with high capacity and low error rate”, in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp: 1729 – 1732, 2008.

[9] “audio steg: overview”, Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/overview.html.

[10] Gary C. Kessler, “Steganography: Hiding Data WithinData”,http://www.garykessler.net/library/steganography.html, September 2001.

[11] C. Parthasarathy and Dr. S.K.Srivatsa, “Increased Robustness Of Lsb Audio Steganography By Reduced Distortion Lsb Coding” 2005. www.jatit.org/volumes/research papers/Vol7No1/9Vol7No1.pdf,

[12] Dr.H.B.Kekre and A.A.Archana, “Information hiding using LSB technique with increased capacity”, International Journal of Cryptography and Security, vol. 1, No.2, October 2008.